Association for Women in Mathematics Series

Jennifer S. Balakrishnan
Amanda Folsom
Matilde Lalín
Michelle Manes *Editors*

Research Directions in Number Theory

Women in Numbers IV

Springer

Association for Women in Mathematics Series

Volume 19

Association for Women in Mathematics Series

Focusing on the groundbreaking work of women in mathematics past, present, and future, Springer's Association for Women in Mathematics Series presents the latest research and proceedings of conferences worldwide organized by the Association for Women in Mathematics (AWM). All works are peer-reviewed to meet the highest standards of scientific literature, while presenting topics at the cutting edge of pure and applied mathematics. Since its inception in 1971, The Association for Women in Mathematics has been a non-profit organization designed to help encourage women and girls to study and pursue active careers in mathematics and the mathematical sciences and to promote equal opportunity and equal treatment of women and girls in the mathematical sciences. Currently, the organization represents more than 3000 members and 200 institutions constituting a broad spectrum of the mathematical community, in the United States and around the world.

More information about this series at http://www.springer.com/series/13764

Jennifer S. Balakrishnan • Amanda Folsom
Matilde Lalín • Michelle Manes
Editors

Research Directions in Number Theory

Women in Numbers IV

Springer

Editors

Jennifer S. Balakrishnan
Department of Mathematics and Statistics
Boston University
Boston, MA, USA

Amanda Folsom
Department of Mathematics and Statistics
Amherst College
Amherst, MA, USA

Matilde Lalín
Département de mathématiques et de statistique
Université de Montréal
Montréal, QC, Canada

Michelle Manes
Department of Mathematics
University of Hawai'i
Honolulu, HI, USA

ISSN 2364-5733 ISSN 2364-5741 (electronic)
Association for Women in Mathematics Series
ISBN 978-3-030-19477-2 ISBN 978-3-030-19478-9 (eBook)
https://doi.org/10.1007/978-3-030-19478-9

Mathematics Subject Classification: 05C25, 14G50, 11G20

This Springer imprint is published by the registered company Springer Nature Switzerland AG.
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

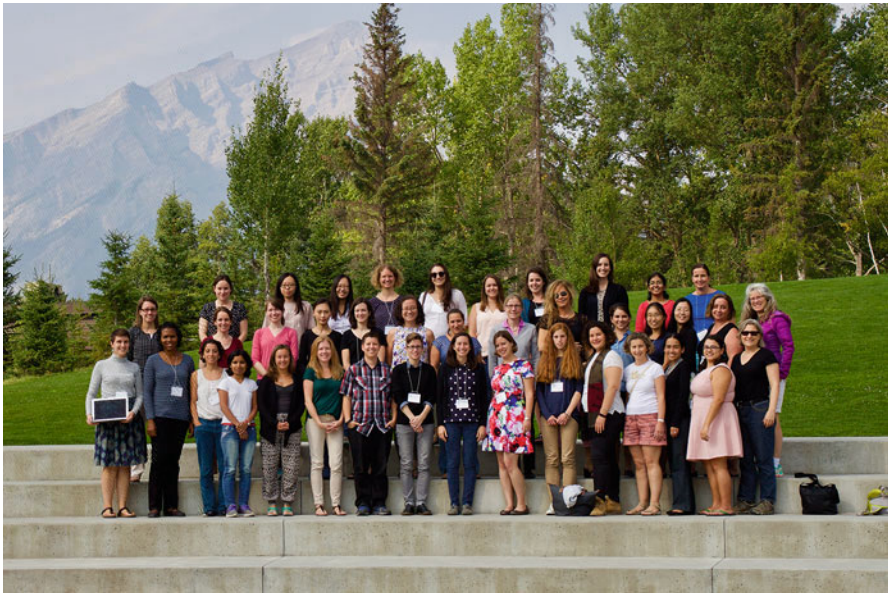

Fig. 1 Conference photo, courtesy of Banff International Research Station

Preface

This volume is a compilation of research and survey papers in number theory, written by members of the Women in Numbers (WIN) network, principally by the collaborative research groups formed at Women in Numbers 4 (WIN4), a conference at the Banff International Research Station in Banff, Alberta, on August 14–18, 2017.

The WIN conference series began in 2008. The series introduced a novel research-mentorship model: women at all career stages, from graduate students to senior members of the community, joined forces to work in focused research groups on cutting-edge projects designed and led by experienced researchers. This model has proven so successful that to date there are nearly 20 research networks for women in mathematics, each of which holds Research Collaboration Conferences for Women as well as other conferences, workshops, special sessions, and symposia. The Association for Women in Mathematics (AWM), funded by the National Science Foundation ADVANCE program, is now supporting and researching the effectiveness of this research-mentorship model (https://awmadvance.org/rccws/).

The goals for WIN4 were to generate research in significant topics in number theory; to broaden the research programs of women and gender minorities working in number theory, especially pre-tenure; to train graduate students and postdocs in number theory by providing experience with collaborative research and the publication process; to strengthen and extend a research network of potential collaborators in number theory and related fields; to enable faculty at small colleges to participate actively in research activities including mentoring graduate students and postdocs; and to highlight research activities of women in number theory.

The majority of the week was devoted to research activities. Before the conference, the participants were organized into nine project groups by research interest and asked to learn background for their project topics. During the workshop, the group leaders gave short talks to all the participants introducing their general areas of research and their groups' projects. On the final day, the group members described their progress and shared their plans to complete the work.

Forty-two mathematicians attended the WIN4 workshop, which was organized by Editors Balakrishnan and Manes along with Chantal David (Concordia University) and Bianca Viray (University of Washington).

The editors solicited contributions from the working groups at the WIN4 workshop and sought additional articles through the Women in Numbers Network (mailing list and web site). All submissions to this volume were sent to anonymous referees, who assessed the work as correct and worthwhile contributions to these proceedings. This volume is the sixth proceedings released after a WIN conference.

The articles collected here span algebraic, analytic, and computational areas of number theory, including topics such as elliptic and hyperelliptic curves, mock modular forms, arithmetic dynamics, and cryptographic applications. Several papers in this volume stem from collaborations between authors with different mathematical backgrounds, allowing the group to tackle a problem using multiple perspectives and tools. In what follows, we highlight some connections between the articles in this volume and also the subjects covered.

Bridging the areas of number theory and cryptography is the article *Ramanujan Graphs in Cryptography* (Costache et al.). From the perspective of both subjects, this paper studies the security of a proposal for post-quantum cryptography.

Four papers in this volume surround computational aspects of curves, varieties, and surfaces. *Computational Aspects of Supersingular Elliptic Curves* (Bank et al.) studies the problem of generating the endomorphism ring of a supersingular elliptic curve by two cycles in ℓ-isogeny graphs, while *Chabauty-Coleman Experiments on Genus Three Hyperelliptic Curves* (Balakrishnan et al.) describes a computation of rational points on genus three hyperelliptic curves defined over $\mathbb{Q}$ whose Jacobians have Mordell-Weil rank 1. *Weierstrass Equations for the Elliptic Fibrations of a K3 Surface* (Lecacheux) concludes a study of the classification of elliptic fibrations of a singular $K3$ surface by giving all Weierstrass equations. Lastly, within this theme, *Newton Polygons of Cyclic Covers of the Projective Line* (Li et al.) applies the Shimura-Taniyama method for computing the Newton polygon of an abelian variety with complex multiplication to cyclic covers of the projective line branched at three points and produces multiple new examples.

Arithmetic dynamics is another subject explored in multiple papers and from different standpoints: *Arithmetic Dynamics and Galois Representations* (Juul et al.) proves a version of Jones' conjectures on the arboreal representation of a degree two rational map, and *Dessins d'enfants for Single-Cycle Belyi Maps* (Manes et al.) describes the dessins d'enfants for two infinite families of dynamical Belyi maps, completing a correspondence given by Riemann's existence theorem.

The last two papers in this volume are in the areas of algebraic number theory, *Multiplicative Order and Frobenius Symbol for the Reductions of Number Fields* (Perucca) and, analytic number theory, *Quantum Modular Forms and Singular Combinatorial Series with Distinct Roots of Unity* (Folsom et al.); the former studies the density of a set of primes of a number field which is defined by some conditions concerning the reductions of algebraic numbers, and the latter establishes the quantum modularity of the $(n + 1)$-variable combinatorial rank generating function for n-marked Durfee symbols.

Workshop Project Titles

WIN4 was a working conference, with several hours each day devoted to research in project groups.

- Apollonian circle packings
  Group members: Holley Friedlander, Elena Fuchs, Piper H, Catherine Hsu, Damaris Schindler, Katherine Stange
- Arithmetic dynamics and Galois representations
  Group members: Jamie Juul, Holly Krieger, Nicole Looper, Michelle Manes, Bianca Thompson, Laura Walton
- Chabauty-Coleman experiments on genus three hyperelliptic curves
  Group members: Jennifer S. Balakrishnan, Francesca Bianchi, Victoria Cantoral-Farfán, Mirela Çiperiani, Anastassia Etropolski
- Computational aspects of supersingular elliptic curves
  Group members: Efrat Bank, Catalina Camacho, Kirsten Eisenträger, Jennifer Park
- Horizontal distribution questions for elliptic curves over $\mathbb{Q}$
  Group members: Chantal David, Ayla Gafni, Amita Malik, Lillian Pierce, Neha Prabhu, Caroline Turnage-Butterbaugh
- Newton polygons of cyclic covers of the projective line
  Group members: Wanlin Li, Elena Mantovan, Rachel Pries, Yunqing Tang
- Quantum modular forms and singular combinatorial series
  Group members: Amanda Folsom, Min-Joo Jang, Sam Kimport, Holly Swisher
- Ramanujan graphs in Cryptography
  Group members: Anamaria Costache, Brooke Feigon, Kristin Lauter, Maike Massierer, Anna Puskás
- Torsion structures on elliptic curves
  Group members: Abbey Bourdon, Özlem Ejder, Yuan Liu, Frances Odumodu, Bianca Viray

Participants and Affiliations at the Time of the Workshop

Jennifer S. Balakrishnan, Boston University, USA
Efrat Bank, University of Michigan, USA
Francesca Bianchi, University of Oxford, UK
Abbey Bourdon, University of Georgia, USA
Ana Catalina Camacho Navarro, Colorado State University, USA
Victoria Cantoral Farfán, ICTP, Italy

Mirela Çiperiani, The University of Texas at Austin, USA
Anamaria Costache, University of Bristol, UK
Chantal David, Concordia University, Canada
Kirsten Eisenträger, The Pennsylvania State University, USA
Özlem Ejder, University of Southern California, USA
Anastassia Etropolski, Rice University, USA
Brooke Feigon, The City College of New York (CUNY), USA
Amanda Folsom, Amherst College, USA
Holley Friedlander, Dickinson College, USA
Elena Fuchs, University of California, Davis, USA
Ayla Gafni, University of Rochester, USA
Piper H, University of Hawai‘i at Mānoa, USA
Catherine Hsu, University of Oregon, USA
Min-Joo Jang, University of Cologne, Germany
Jamie Juul, Amherst College, USA
Sam Kimport, Stanford University, USA
Holly Krieger, University of Cambridge, UK
Kristin Lauter, Microsoft Research, USA
Wanlin Li, University of Wisconsin-Madison, USA
Yuan Liu, University of Wisconsin-Madison, USA
Nicole Looper, Northwestern University, USA
Amita Malik, University of Illinois at Urbana-Champaign, USA
Michelle Manes, University of Hawai‘i at Mānoa, USA
Elena Mantovan, California Institute of Technology, USA
Maike Massierer, University of New South Wales, Sydney, Australia
Frances Odumodu, Université Bordeaux, France
Jennifer Park, University of Michigan, USA
Lillian Pierce, Duke University, USA
Neha Prabhu, Indian Institute of Science Education and Research-Pune, India
Rachel Pries, Colorado State University, USA
Anna Puskás, University of Alberta, Canada
Damaris Schindler, Utrecht University, The Netherlands
Katherine Stange, University of Colorado Boulder, USA
Holly Swisher, Oregon State University, USA
Yunqing Tang, IAS/Princeton University, USA
Bianca Thompson, Harvey Mudd College, USA
Caroline Turnage-Butterbaugh, Duke University, USA
Bianca Viray, University of Washington, USA
Laura Walton, Brown University, USA

Workshop Website

https://www.birs.ca/events/2017/5-day-workshops/17w5083

Boston, MA, USA	Jennifer S. Balakrishnan
Amherst, MA, USA	Amanda Folsom
Montréal, QC, Canada	Matilde Lalín
Honolulu, HI, USA	Michelle Manes
March 2019	

Acknowledgments

We are grateful to the following sponsoring organizations for their support of the workshop and this volume:

- Banff International Research Station
- National Science Foundation (DMS 1712938)
- Clay Mathematics Institute
- Microsoft Research
- The Number Theory Foundation
- Pacific Institute for the Mathematical Sciences
- Association for Women in Mathematics and the AWM ADVANCE Grant (NSF HRD 1500481)

We would like to thank the referees whose careful and dedicated work have been crucial in assuring the quality of this publication.

Contents

List of Contributors

Jennifer S. Balakrishnan Department of Mathematics and Statistics, Boston University, 111 Cummington Mall, Boston, MA 02215, USA, e-mail: jbala@bu.edu

Efrat Bank Department of Mathematics, University of Michigan, Ann Arbor, MI, USA, e-mail: ebank@umich.edu

Francesca Bianchi Mathematical Institute, University of Oxford, Andrew Wiles Building, Radcliffe Observatory Quarter, Woodstock Road, Oxford OX2 6GG, UK, e-mail: francesca.bianchi@maths.ox.ac.uk

Catalina Camacho-Navarro Department of Mathematics, Colorado State University, Fort Collins, CO 80523, USA, e-mail: camacho@math.colostate.edu

Victoria Cantoral-Farfán The Abdus Salam International Center for Theoretical Physics, Mathematics Section, 11 Strada Costiera, 34151 Trieste, Italy, e-mail: vcantora@ictp.it

Mirela Çiperiani Department of Mathematics, The University of Texas at Austin, 1 University Station, C1200, Austin, TX 78712, USA, e-mail: mirela@math.utexas.edu

Anamaria Costache Department of Computer Science, University of Bristol, Bristol, UK, e-mail: anamaria.costache@bristol.ac.uk

Kirsten Eisenträger Department of Mathematics, The Pennsylvania State University, University Park, PA 16802, USA, e-mail: eisentra@math.psu.edu

Anastassia Etropolski Department of Mathematics, Rice University MS 136, Houston, TX 77251, USA, e-mail: aetropolski@rice.edu

Brooke Feigon Department of Mathematics, The City College of New York, CUNY, NAC 8/133, New York, NY 10031, USA, e-mail: bfeigon@ccny.cuny.edu

Amanda Folsom Department of Mathematics and Statistics, Amherst College, Amherst, MA 01002, USA, e-mail: afolsom@amherst.edu

Min-Joo Jang Department of Mathematics, The University of Hong Kong, Room 318, Run Run Shaw Building, Pokfulam, Hong Kong, e-mail: min-joo.jang@hku.hk

Jamie Juul Department of Mathematics, The University of British Columbia, 1984 Mathematics Road, Vancouver, BC V6T 1Z2, Canada, e-mail: jamie.l.rahr@gmail.com

Sam Kimport Department of Mathematics, Stanford University, 450 Serra Mall, Building 380, Stanford, CA 94305, USA, e-mail: skimport@stanford.edu

Holly Krieger Department of Pure Mathematics and Mathematical Statistics, University of Cambridge, Wilberforce Road, Cambridge CB3 0WB, UK, e-mail: hkrieger@dpmms.cam.ac.uk

Kristin Lauter Microsoft Research, One Microsoft Way, Redmond, WA 98052, USA, e-mail: klauter@microsoft.com

Odile Lecacheux Sorbonne Université, Institut de Mathématiques de Jussieu-Paris Rive Gauche, 4 Place Jussieu, 75252 Paris Cedex 05, France, e-mail: odile.lecacheux@imj-prg.fr

Wanlin Li Department of Mathematics, University of Wisconsin, Madison, WI 53706, USA, e-mail: wanlin@math.wisc.edu

Nicole Looper Department of Pure Mathematics and Mathematical Statistics, University of Cambridge, Wilberforce Road, Cambridge CB3 0WB, UK, e-mail: nl393@cam.ac.uk

Michelle Manes Department of Mathematics, University of Hawai‘i at Mānoa, 2565 McCarthy Mall Keller 401A, Honolulu, HI 96822, USA, e-mail: mmanes@math.hawaii.edu

Elena Mantovan Department of Mathematics, California Institute of Technology, Pasadena, CA 91125, USA, e-mail: mantovan@caltech.edu

Maike Massierer School of Mathematics and Statistics, University of New South Wales, Sydney, NSW 2052, Australia

Gabrielle Melamed Department of Mathematics, University of Connecticut, 341 Mansfield Road U1009, Storrs, CT 06269, USA, e-mail: Gabrielle.Melamed@uconn.edu

Travis Morrison Institute for Quantum Computing, The University of Waterloo, Waterloo, ON, Canada, e-mail: travis.morrison@uwaterloo.ca

Jennifer Park Department of Mathematics, University of Michigan, Ann Arbor, MI, USA, e-mail: jmypark@umich.edu

Antonella Perucca University of Luxembourg, Mathematics Research Unit, 6, avenue de la Fonte L-4364, Esch-sur-Alzette, Luxembourg, e-mail: antonella.perucca@uni.lu

Rachel Pries Department of Mathematics, Colorado State University, Fort Collins, CO 80523, USA, e-mail: pries@math.colostate.edu

Anna Puskás Department of Mathematics & Statistics, University of Massachusetts, Amherst, MA 01003, USA, e-mail: anna.puskas@ipmu.jp

Holly Swisher Department of Mathematics, Oregon State University, Kidder Hall 368, Corvallis, OR 97331, USA, e-mail: swisherh@math.oregonstate.edu

Yunqing Tang Department of Mathematics, Princeton University, Princeton, NJ 08540, USA, e-mail: yunqingt@math.princeton.edu

Bianca Thompson Westminster College, Salt Lake City, UT 84105, USA, e-mail: bthompson@westminstercollege.edu

Bella Tobin Department of Mathematics, University of Hawai'i at Mānoa, 2565 McCarthy Mall Keller 401A, Honolulu, HI 96822, USA, e-mail: tobin@math.hawaii.edu; bellatobin@gmail.com

Laura Walton Mathematics Department, Brown University, Providence, RI 02912, USA, e-mail: laura@math.brown.edu

Ramanujan Graphs in Cryptography

Anamaria Costache, Brooke Feigon, Kristin Lauter, Maike Massierer, and Anna Puskás

Abstract In this paper we study the security of a proposal for Post-Quantum Cryptography from both a number theoretic and cryptographic perspective. Charles–Goren–Lauter in 2006 proposed two hash functions based on the hardness of finding paths in Ramanujan graphs. One is based on Lubotzky–Phillips–Sarnak (LPS) graphs and the other one is based on Supersingular Isogeny Graphs. A 2008 paper by Petit–Lauter–Quisquater breaks the hash function based on LPS graphs. On the Supersingular Isogeny Graphs proposal, recent work has continued to build cryptographic applications on the hardness of finding isogenies between supersingular elliptic curves. A 2011 paper by De Feo–Jao–Plût proposed a cryptographic system based on Supersingular Isogeny Diffie–Hellman as well as a set of five hard problems. In this paper we show that the security of the SIDH proposal relies on

Brooke Feigon was partially supported by National Security Agency grant H98230-16-1-0017 and PSC-CUNY.
Maike Massierer was partially supported by Australian Research Council grant DP150101689.

A. Costache
Department of Computer Science, University of Bristol, Bristol, UK
e-mail: anamaria.costache@bristol.ac.uk

B. Feigon (✉)
Department of Mathematics, The City College of New York, CUNY, NAC 8/133, New York, NY 10031, USA
e-mail: bfeigon@ccny.cuny.edu

K. Lauter
Microsoft Research, One Microsoft Way, Redmond, WA 98052, USA
e-mail: klauter@microsoft.com

M. Massierer
School of Mathematics and Statistics, University of New South Wales, Sydney, NSW 2052, Australia

A. Puskás
Department of Mathematics & Statistics, University of Massachusetts, Amherst, MA 01003, USA
e-mail: anna.puskas@ipmu.jp

J. S. Balakrishnan et al. (eds.), *Research Directions in Number Theory*, Association for Women in Mathematics Series 19, https://doi.org/10.1007/978-3-030-19478-9_1

the hardness of the SSIG path-finding problem introduced in Charles et al. (2009). In addition, similarities between the number theoretic ingredients in the LPS and Pizer constructions suggest that the hardness of the path-finding problem in the two graphs may be linked. By viewing both graphs from a number theoretic perspective, we identify the similarities and differences between the Pizer and LPS graphs.

Keywords Post-Quantum Cryptography · Supersingular isogeny graphs · Ramanujan graphs

2010 Mathematics Subject Classification Primary: 14G50, 11F70; Secondary: 05C75, 11R52

1 Introduction

Supersingular Isogeny Graphs were proposed for use in cryptography in 2006 by Charles, Goren, and Lauter [3]. Supersingular isogeny graphs are examples of Ramanujan graphs, i.e., optimal expander graphs. This means that relatively *short* walks on the graph approximate the uniform distribution, i.e., walks of length approximately equal to the logarithm of the graph size. Walks on expander graphs are often used as a good source of randomness in computer science, and the reason for using *Ramanujan* graphs is to keep the path length short. But the reason these graphs are important for cryptography is that *finding paths* in these graphs, i.e., *routing,* is hard: there are no known subexponential algorithms to solve this problem, either classically or on a quantum computer. For this reason, systems based on the hardness of problems on Supersingular Isogeny Graphs are currently under consideration for standardization in the NIST Post-Quantum Cryptography (PQC) Competition [21].

Charles et al. [3] proposed a general construction for cryptographic hash functions based on the hardness of inverting a walk on a graph. The path-finding problem is the following: given fixed starting and ending vertices representing the start and end points of a walk on the graph of a fixed length, find a path between them. A hash function can be defined by using the input to the function as directions for walking around the graph: the output is the label for the ending vertex of the walk. Finding collisions for the hash function is equivalent to finding cycles in the graph, and finding preimages is equivalent to path-finding in the graph. Backtracking is not allowed in the walks by definition, to avoid trivial collisions.

In [3], two concrete examples of families of optimal expander graphs (Ramanujan graphs) were proposed, the so-called Lubotzky–Phillips–Sarnak (LPS) graphs [14], and the Supersingular Isogeny Graphs (Pizer) [20], where the path-finding problem was supposed to be hard. Both graphs were proposed and presented at the 2005 and 2006 NIST Hash Function workshops, but the LPS hash function was quickly attacked and broken in two papers in 2008, a collision attack [24] and a preimage attack [17]. The preimage attack gives an algorithm to efficiently find paths in LPS graphs, a problem which had been open for several decades. The PLQ path-finding algorithm uses the explicit description of the graph as a Cayley graph in $\mathrm{PSL}_2(\mathbb{F}_p)$, where vertices are 2×2 matrices with entries in $\mathbb{F}_p$ satisfying certain properties. Given the swift discovery of attacks on the LPS path-finding problem, it is natural to investigate whether this approach is relevant to the path-finding problem in Supersingular Isogeny (Pizer) Graphs.

In 2011, De Feo–Jao–Plût [8] devised a cryptographic system based on supersingular isogeny graphs, proposing a Diffie–Hellman protocol as well as a set of five hard problems related to the security of the protocol. It is natural to ask what is the relation between the problems stated in [8] and the path-finding problem on Supersingular Isogeny Graphs proposed in [3].

In this paper we explore these two questions related to the security of cryptosystems based on these Ramanujan graphs. In Part 1 of the paper, we study the relation between the hard problems proposed by De Feo–Jao–Plût and the hardness of the Supersingular Isogeny Graph problem which is the foundation for the CGL hash function. In Part 2 of the paper, we study the relation between the Pizer and LPS graphs by viewing both from a number theoretic perspective.

In particular, in Part 1 of the paper, we clearly explain how the security of the Key-Exchange protocol relies on the hardness of the path-finding problem in SSIG, proving a reduction (Theorem 3.2) between the Supersingular Isogeny Diffie Hellmann (SIDH) Problem and the path-finding problem in SSIG. Although this fact and this theorem may be clear to the experts (see, for example, the comment in the introduction to a recent paper on this topic [1]), this reduction between the hard problems is not written anywhere in the literature. Furthermore, the Key-Exchange (SIDH) paper [8] states 5 hard problems, including (SSCDH), with relations proved between some but not all of them, and mentions the paper [3] only in passing (on page 17), with no clear statement of the relationship to the overarching hard problem of path-finding in SSIG.

Our Theorem 3.2 clearly shows the fact that the security of the proposed post-quantum key-exchange relies on the hardness of the path-finding problem in SSIG stated in [3]. Theorem 4.9 counts the chains of isogenies of fixed length. Its proof relies on elementary group theory results and facts about isogenies, proved in Section 4.

In Part 2 of the paper, we examine the LPS and Pizer graphs from a number theoretic perspective with the aim of highlighting the similarities and differences between the constructions.

Both the LPS and Pizer graphs considered in [3] can be thought of as graphs on

$$\Gamma \backslash \mathrm{PGL}_2(\mathbb{Q}_l)/\mathrm{PGL}_2(\mathbb{Z}_l), \tag{1}$$

where Γ is a discrete cocompact subgroup, where Γ is obtained from a quaternion algebra B. We show how different input choices for the construction lead to different graphs. In the LPS construction one may vary Γ to get an infinite family of Ramanujan graphs. In the Pizer construction one may vary B to get an infinite family. In the LPS case, we always work in the Hamiltonian quaternion algebra. For this particular choice of algebra we can rewrite the graph as a Cayley graph. This explicit description is key for breaking the LPS hash function. For the Pizer graphs we do not have such a description. On the Pizer side the graphs may, via Strong Approximation, be viewed as graphs on adèlic double cosets which are in turn the class group of an order of B that is related to the cocompact subgroup Γ. From here one obtains an isomorphism with supersingular isogeny graphs. For LPS graphs the local double cosets are also isomorphic to adèlic double cosets, but in this case the corresponding set of adèlic double cosets is smaller relative to the quaternion algebra and we do not have the same chain of isomorphisms.

Part 2 has the following outline. Section 6 follows [15] and presents the construction of LPS graphs from three different perspectives: as a Cayley graph, in terms of local double cosets, and, to connect these two, as a quotient of an infinite tree. The edges of the LPS graph are explicit in both the Cayley and local double coset presentation. In Section 6.4 we give an explicit bijection between the natural parameterizations of the edges at a fixed vertex. Section 7 is about Strong Approximation, the main tool connecting the local and adelic double cosets for both LPS and Pizer graphs. Section 8 follows [20] and summarizes Pizer's construction. The different input choices for LPS and Pizer constructions impose different restrictions on the parameters of the graph, such as the degree. 6-regular graphs exist in both families. In Section 8.2 we give a set of congruence conditions for the parameters of the Pizer construction that produce a 6-regular graph. In Section 9 we summarize the similarities and differences between the two constructions.

1.1 Acknowledgments

This project was initiated at the Women in Numbers 4 (WIN4) workshop at the Banff International Research Station in August, 2017. The authors would like to thank BIRS and the WIN4 organizers. In addition, the authors would like to thank the Clay Mathematics Institute, PIMS, Microsoft Research, the Number Theory Foundation, and the NSF-HRD 1500481—AWM ADVANCE grant for supporting the workshop. We thank John Voight, Scott Harper, and Steven Galbraith for helpful conversations, and the anonymous referees for many helpful suggestions and edits.

Part 1: Cryptographic Applications of Supersingular Isogeny Graphs

In this section we investigate the security of the [8] key-exchange protocol. We show a reduction to the path-finding problem in supersingular isogeny graphs stated in [3]. The hardness of this problem is the basis for the CGL cryptographic hash function, and we show here that if this problem is not hard, then the key exchange presented in [8] is not secure.

We begin by recalling some basic facts about isogenies of elliptic curves and the key-exchange construction. Then, we give a reduction between two hardness assumptions. This reduction is based on a correspondence between a path representing the composition of m isogenies of degree ℓ and an isogeny of degree ℓ^m.

2 Preliminaries

We start by recalling some basic and well-known results about isogenies. They can all be found in [23]. We try to be as concrete and constructive as possible, since we would like to use these facts to do computations.

An elliptic curve is a curve of genus one with a specific base point $\mathcal{O}$. This latter can be used to define a group law. We will not go into the details of this, see, for example, [23]. If E is an elliptic curve defined over a field K and $\mathrm{char}(\bar{K}) \neq 2, 3$, we can write the equation of E as

$$E : y^2 = x^3 + a \cdot x + b,$$

where $a, b \in K$. Two important quantities related to an elliptic curve are its discriminant Δ and its j-invariant, denoted by j. They are defined as follows:

$$\Delta = 16 \cdot (4 \cdot a^3 + 27 \cdot b^2) \quad \text{and} \quad j = -1728 \cdot \frac{a^3}{\Delta}.$$

Two elliptic curves are isomorphic over $\bar{K}$ if and only if they have the same j-invariant.

Definition 2.1. *Let E_0 and E_1 be two elliptic curves. An isogeny from E_0 to E_1 is a surjective morphism*

$$\phi : E_0 \to E_1,$$

which is a group homomorphism.

An example of an isogeny is the multiplication-by-m map $[m]$,

$$\begin{aligned} [m] : E &\to E \\ P &\mapsto m \cdot P. \end{aligned}$$

The degree of an isogeny is defined as the degree of the finite extension $\bar{K}(E_0)/\phi^*(\bar{K}(E_1))$, where $\bar{K}(*)$ is the function field of the curve, and ϕ^* is the map of function fields induced by the isogeny ϕ. By convention, we set